

# SEMICHARACTERS OF GROUPS

GIL ALON

**ABSTRACT.** We define the notion of a semicharacter of a group  $G$ : A function from the group to  $\mathbb{C}^*$ , whose restriction to any abelian subgroup is a homomorphism. We conjecture that for any finite group, the order of the group of semicharacters is divisible by the order of the group. We prove that the conjecture holds for some families of groups, including the symmetric and general linear groups.

## 1. INTRODUCTION

If  $G$  is a finite abelian group, the dual group  $\widehat{G} = \text{Hom}(G, \mathbb{C}^*)$  is isomorphic to  $G$ . For a general finite group  $G$ ,  $\text{Hom}(G, \mathbb{C}^*)$  may provide less information about the group: For example, when  $G$  is simple and nonabelian,  $\text{Hom}(G, \mathbb{C}^*) = \{1\}$ . As representation theory suggests, one has to look at homomorphisms to matrix groups  $GL_n(\mathbb{C})$  to recover more information about the group.

In this paper we take a different approach: Instead of replacing  $\mathbb{C}^*$  with a larger group, we alleviate somewhat the homomorphism condition. Let us call a function  $f : G \rightarrow \mathbb{C}^*$  a *semicharacter* if it satisfies  $f(ab) = f(a)f(b)$  for all pairs  $a, b \in G$  of *commuting* elements. In other words, a semicharacter on  $G$  is a function whose restriction to any abelian subgroup is a character.

The set of semicharacters of  $G$ , with the operation of pointwise multiplication, is an abelian group. Let us denote this group by  $\widehat{G}$ , as this notation is consistent with the case where  $G$  is abelian.

It is easy to see (lemma 2.2) that  $\widehat{G}$  is always finite. In this paper we will be interested in the relation between order of  $\widehat{G}$  and the order of  $G$ . We make the following conjecture:

**Conjecture 1.1.** *For any finite group  $G$ ,  $|\widehat{G}|$  is divisible by  $|G|$ .*

This conjecture is based on some evidence: for abelian groups, it is obviously true. For groups of very small order, it can be verified by a direct calculation. Using the computer algebra system **GAP** and the **SmallGroups** library, we have verified it for all groups of order  $\leq 255$ .

In addition, we will prove that the conjecture holds for the following families of groups:

- The Symmetric groups (theorem 4.2).

---

2000 *Mathematics Subject Classification.* 20D99.

- The Alternating groups (theorem 4.5).
- The linear groups  $GL(n, q)$  (theorem 6.6).
- The groups  $SL(n, q)$  when  $(n, q - 1) = 1$  (in which case,  $SL(n, q) = PSL(n, q)$ ) - corollary 6.7.
- The upper triangular unipotent groups  $U(n, q)$  when  $q = p^e$  and  $p > n$  (lemma 2.7).
- The Dihedral groups (theorem 5.3).

We will prove all these statements by constructing semicharacters explicitly. Our interest in conjecture 1.1 stems mainly from the variety of techniques that can be applied for the construction of semicharacters, and which seem to provide some insight into the structure of the group.

As an example, let us look at the Heisenberg group over a finite field  $\mathbb{F}$ . Consider the three functions from the group to the additive group  $\mathbb{F}^+$ , defined by

$$f_1 \left( \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \right) = a; \quad f_2 \left( \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \right) = c; \quad f_3 \left( \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \right) = ac - 2b$$

$f_1$  and  $f_2$  are group homomorphisms.  $f_3$  is not a homomorphism, but it satisfies  $f(AB) = f(A) + f(B)$  whenever  $A$  and  $B$  commute, as can be verified directly. By taking linear combinations of these 3 functions, and composing them with a homomorphism from  $\mathbb{F}^+$  to  $\mathbb{C}^*$ , we get enough semicharacters on the group.

In the proof of theorem 5.3, we will generalize this construction to upper triangular unipotent matrices via a discrete version of the log function.

For groups whose order is not a prime power, we consider the  $l$ -part of  $\widehat{G}$  separately for each prime divisor  $l$  of  $|G|$ . The  $l$ -part depends only on the  $l$ -Sylow subgroups and their intersection pattern (see lemma 2.5). For the symmetric group, we will construct semicharacters using the cycle decomposition of permutations. Basically, one is free to define the value of a semicharacter in the  $l$ -torsion part of  $\widehat{S}_n$  on cycles of maximal  $l$ -power size. For the linear groups  $GL(n, p^t)$ , and  $l \neq p$ , we will make a similar construction, with cycles of maximal  $l$ -power size replaced by transformations of maximal  $l$ -power order on irreducible invariant spaces of maximal dimension. At  $l = p$  our construction is similar to the case of the unipotent groups.

We will also prove, for a general group  $G$ , that  $\widehat{G} \neq \{0\}$  if  $G \neq \{1\}$  (see theorem 3.1). For that, we will use the nontrivial fact that any simple group has a cyclic Sylow subgroup.

## 2. SOME NOTATION AND LEMMAS

All the groups in this paper are assumed to be finite. We repeat the definitions in the introduction:

**Definition 2.1.** (1) A *semicharacter* on a group  $G$  is a function  $f : G \rightarrow \mathbb{C}^*$  satisfying  $f(ab) = f(a)f(b)$  for all pairs  $a, b \in G$  of commuting elements.

(2) The group of semicharacters of  $G$  is denoted by  $\widehat{G}$ .

We obtain a contravariant functor  $\widehat{\phantom{x}}$  from groups to abelian groups, sending a group  $G$  to  $\widehat{G}$ , and a group homomorphism  $\phi : G \rightarrow H$  to the homomorphism  $\widehat{\phi} : \widehat{H} \rightarrow \widehat{G}$  defined by  $\widehat{\phi}(f) = f \circ \phi$ .

**Lemma 2.2.** *For any  $G$ ,  $\widehat{G}$  is a finite abelian group, and its order divides  $\prod_{g \in G} \text{ord}(g)$ .*

*Proof.* If  $\phi \in \widehat{G}$  then for every  $g \in G$ ,  $\phi(g)^{\text{ord}(g)} = \phi(g^{\text{ord}(g)}) = 1$ . The result follows immediately.  $\square$

**Definition 2.3.** For any group  $G$ , and any prime number  $l$ , we denote by  $G[l^\infty]$  the set of elements whose order is a power of  $l$ , and by  $G[l]$  the set  $\{g \in G \mid g^l = id\}$ .

If  $G$  is abelian, then  $G[l^\infty]$  and  $G[l]$  are subgroups of  $G$ . We have

$$\widehat{G} = \prod_l \widehat{G}[l^\infty]$$

And each  $\widehat{G}[l^\infty]$  is of  $l$ -power size. We will now see that  $\widehat{G}[l^\infty]$  depends only on the elements of  $G[l^\infty]$  and their multiplication table.

**Definition 2.4.** We denote by  $\widehat{G[l^\infty]}$  the group of maps  $f : G[l^\infty] \rightarrow \mathbb{C}^*$  such that  $f(xy) = f(x)f(y)$  whenever  $x, y$  are commuting elements in  $G[l^\infty]$ .

Note that a function  $f : G[l^\infty] \rightarrow \mathbb{C}^*$  is in  $\widehat{G[l^\infty]}$  if and only if for any  $l$ -Sylow subgroup  $L \leq G$ ,  $f|_L \in \widehat{L}$ .

**Lemma 2.5.** *The restriction map from  $\widehat{G}[l^\infty]$  to  $\widehat{G[l^\infty]}$  is an isomorphism.*

*Proof.* We have to prove that each function in  $\widehat{G[l^\infty]}$  has a unique extension to  $G$  which is in  $\widehat{G}[l^\infty]$ . Let  $|G| = nl^a$  with  $l \nmid n$ , and let  $b \in \mathbb{Z}$  be such that  $bn \equiv 1 \pmod{l^a}$ . Then  $\tilde{f}(g) = f(g^n)^b$  is the required extension of  $f$ . The extension is unique because any  $f \in \widehat{G}[l^\infty]$  satisfies  $f(g) = f(g^n)^b$ .  $\square$

Lemma 2.5 will be our main tool for constructing semicharacters on groups.

*Remark 2.6.* It follows from lemma 2.5 that  $\widehat{G}[l] \cong \widehat{G[l^\infty]}[l]$ . We will view elements of the right hand side as functions  $f : G[l^\infty] \rightarrow \mathbb{F}_l^+$  satisfying  $f(ab) = f(a) + f(b)$  if  $ab = ba$ . It follows that if we can find  $d$  such functions which are linearly independent over  $\mathbb{F}_l$ , then  $|\widehat{G}|$  is divisible by  $l^d$ .

We conclude this section with an example: the dihedral groups-

**Lemma 2.7.** *For  $G = D_n = \langle r, s \mid r^n = s^2 = 1, srs^{-1} = r^{-1} \rangle$  we have  $|\widehat{G}| = \begin{cases} n2^n & 2 \nmid n \\ n2^{\frac{n}{2}} & 2 \mid n \end{cases}$ .*

*Proof.* Any semicharacter  $\phi \in \widehat{G}$  sends  $r$  to an  $n$ th root of unity (which determines  $\phi$  on  $r, r^2, \dots, r^{n-1}$ ), and an involution  $sr^i$  to  $\pm 1$ . If  $n$  is odd then each involution commutes only with itself and the identity, hence  $|\widehat{D_n}| = n2^n$ . If  $n$  is even, say  $n = 2m$ , then  $r^m$  is an involution as well, and each involution of the form  $sr^i$  commutes only with  $1, r^m, sr^{i+m}$  and itself. Hence, given the image of  $r$ , we are free to choose the image of  $\phi$  on one of each  $\{sr^i, sr^{i+m}\}$ , and the other image is determined by  $\phi(r)^m = \pm 1$ . We get  $|\widehat{D_n}| = n2^m$ .  $\square$

Thus, Conjecture 1.1 holds for the dihedral groups.

### 3. NONTRIVIALITY

**Theorem 3.1.** *For any finite group  $G \neq 0$ ,  $\widehat{G} \neq 0$ .*

*Proof.* Since a semicharacter on a quotient of  $G$  can be pulled back to  $G$ , we may assume that  $G$  is simple. By [2, Theorem 4.9],  $G$  has a cyclic Sylow subgroup. Let  $L$  be such a subgroup. Let  $|L| = l^r$  for a prime  $l$ . Let  $A = \{g \in G | g^l = 1\}$  and let us write  $a \sim b$  for  $a, b \in A$  if  $b$  is a power of  $a$  and  $\text{ord}(a) = \text{ord}(b)$ . This is an equivalence relation, and thus there exists a nonzero function  $F : A \rightarrow \mathbb{F}_l^+$  satisfying  $F(a^n) = nF(a)$  for  $a \in A, n \in \mathbb{Z}$  such that  $F(a) \neq 0$  if  $a \neq 1$ . In other words,  $F$  is a nonzero homomorphism when restricted to any subgroup of order  $l$ . Let  $m = l^{r-1}$  and define  $f : G[l^\infty] \rightarrow \mathbb{F}_l^+$  by

$$f(g) = F(g^m)$$

If  $g$  and  $h$  are commuting elements in  $G[l^\infty]$  then they belong to a common Sylow  $l$ -subgroup, which is cyclic, hence  $g^m$  and  $h^m$  belong to a common subgroup of order  $l$ . We get:

$$f(gh) = F((gh)^m) = F(g^m h^m) = F(g^m) + F(h^m) = f(g) + f(h).$$

By lemma 2.5,  $f$  may be extended to an element of  $\widehat{G}[l]$ .

Finally,  $f$  is nonzero since for a generator  $a$  of  $L$ ,  $f(a) \neq 0$ .  $\square$

### 4. THE SYMMETRIC AND ALTERNATING GROUPS

For  $G = S_n$ , the primes dividing  $|G|$  are exactly the primes  $l \leq n$ . Let  $l$  be such a prime, and let  $e$  be such that  $l^e \leq n < l^{e+1}$ .

**Lemma 4.1.** *If  $\alpha, \beta \in S_n[l^\infty]$  commute, and if  $\alpha_1$  (resp.  $\beta_1$ ) is an  $l^e$ -cycle in the cycle decomposition of  $\alpha$  (resp.  $\beta$ ), then either  $\alpha_1$  and  $\beta_1$  are disjoint, or each one is a power of the other.*

*Proof.* Since  $\beta^\alpha = \beta$ ,  $\alpha$  acts on the  $l^e$ -cycles of  $\beta$ . Since  $\alpha$  is of  $l$ -power order, all the orbits of this action are of  $l$ -power size, but  $l \cdot l^e > n$ , hence  $\alpha$  fixes each  $l^r$ -cycle of  $\beta$ . In particular,  $\alpha_1$  and  $\beta_1$  commute. The result follows.  $\square$

**Theorem 4.2.** *For all  $n$ , conjecture 1.1 holds for  $S_n$ .*

*Proof.* For any prime  $l \leq n$ , let  $A$  be the set of  $l^e$ -cycles of  $S_n$ , and define  $a \sim b$  if  $b$  is a power of  $a$ . This is an equivalence relation, and we have  $|A/\sim| = \binom{n}{l^e} \frac{(l^e-1)!}{l^e(1-\frac{1}{l})}$ . Let  $V$  be the  $\mathbb{F}_l$ -vector space of functions  $f : A \rightarrow \mathbb{F}_l^+$  satisfying  $f(\pi^i) = i \cdot f(\pi)$  if  $(i, l) = 1$ . Then  $\dim(V) = |A/\sim|$ . For any  $f \in V$ , we extend  $f$  to a function  $\tilde{f} : S_n[l^\infty] \rightarrow \mathbb{F}_l^+$  by  $\tilde{f}(\pi) = \sum_{c \in c(\pi, l^e)} f(c)$ , where  $c(\pi, k)$  is the set of  $k$ -cycles in the cycle decomposition of  $\pi$ . By lemma 4.1,  $\tilde{f}$  is in  $\widehat{S_n[l^\infty]}[l]$ , and by lemma 2.5 it extends to an element of  $\widehat{S_n}[l]$ . Thus,

$$\dim_{F_l} \widehat{S_n}[l] \geq \binom{n}{l^e} \frac{(l^e-1)!}{l^e - l^{e-1}}$$

It remains to prove that the right hand side is not less than the multiplicity of  $l$  in  $n!$ . Indeed,

$$val_l(n!) = \sum_{i \geq 1} \lfloor \frac{n}{l^i} \rfloor < \frac{n}{l-1}$$

If  $n \neq l^e$  then  $\dim_{F_l} \widehat{S_n}[l] \geq n \geq \frac{n}{l-1} > val_l(n!)$ .

If  $n = l^e$  and  $n \geq 6$ , then using the inequality  $(n-1)! \geq n^2$  we get  $\dim_{F_l} \widehat{S_n}[l] \geq \frac{(n-1)!}{n(1-\frac{1}{l})} \geq \frac{n}{l-1}$ .

For  $l^e = n \leq 5$ ,  $\frac{(n-1)!}{n(1-\frac{1}{l})} \geq val_l(n!)$  holds as well.  $\square$

*Remark 4.3.* On cycles of smaller  $l$ -power order, we are not always free to define the image of a semicharacter. Consider for example 2-cycles. The identity  $(12)(34) \cdot (13)(24) = (14)(23)$  holds in the Klein 4-group which is commutative. Hence for any semicharacter  $f$  of  $S_n$ , we have  $\prod_{1 \leq i < j \leq 4} f((ij)) = 1$ . Moreover, we can replace the indices 1, 2, 3, 4 with  $t_1 < t_2 < t_3 < t_4$ , and get a linear equation modulo 2 for the variables  $f((t_i t_j))$ ,  $1 \leq i < j \leq 4$ . We get  $\binom{n}{4}$  equations in  $\binom{n}{2}$  variables. For  $n = 7$  it can be checked that the only solutions are  $f((ij)) \equiv 1$  and  $f((ij)) \equiv -1$ . Thus, the same holds for any  $n \geq 7$ . This also shows that a character on an abelian subgroup  $H$  of a group  $G$  may not always be extended to a semicharacter of  $G$ .

Let us now consider the alternating groups. The embedding  $A_n \rightarrow S_n$  induces a natural restriction map  $R : \widehat{S_n} \rightarrow \widehat{A_n}$ . Obviously, the sign map  $sgn : S_n \rightarrow \{\pm 1\}$  is in the kernel of this map.

**Lemma 4.4.** (1)  $\ker R \subseteq \widehat{S}_n[2]$

(2) If  $n > 1$  is not of the form  $2^k$  or  $2^k + 1$ , then  $\ker R = \{1, \text{sgn}\}$ .

*Proof.* (1) If  $\phi \in \ker R$ , then for  $g \in S_n$ ,  $\phi(g)^2 = \phi(g^2) = 1$ .

(2) By the assumption,  $n \geq 6$ . Let  $\phi \in \ker R$ , then for any  $i \neq j$  we have  $\phi((ij)) = \pm 1$ . Moreover, for distinct  $i, j, k, l$  we have  $\phi((ij))\phi((kl)) = \phi((ij)(kl)) = 1$ , hence  $\phi((ij)) = \phi((kl))$ . From here it is easy to see that  $\phi$  is constant on all the involutions of the form  $(ij)$ . Multiplying if necessary by  $\text{sgn}$ , we may assume that  $\phi((ij)) = 1$  for all  $i \neq j$ . For every  $r$  such that  $2^r \leq n$ , and any  $2^r$ -cycle  $c \in S_n$ , we may find, by the assumption on  $n$ ,  $i$  and  $j$  such that  $(ij)$  is disjoint from  $c$ , hence  $\phi(c(ij)) = 1 \Rightarrow \phi(c) = 1$ . Hence,  $\phi$  is equal to 1 on  $S_n[2^\infty]$ , and by lemma 2.5,  $\phi = 1$ .  $\square$

**Theorem 4.5.** Conjecture 1.1 holds for  $A_n$ .

*Proof.* By part 1 of lemma 4.4, for  $l > 2$  the  $l$ -part of  $\ker R$  is trivial, hence  $|\widehat{A}_n[l^\infty]| = |\widehat{S}_n[l^\infty]|$  and by theorem 4.2,  $\text{val}_l(|\widehat{A}_n|) = \text{val}_l(|\widehat{S}_n|) \geq \text{val}_l(|S_n|) = \text{val}_l(|A_n|)$ . Thus, it remains to prove that  $\text{val}_2(|\widehat{A}_n|) \geq \text{val}_2(|A_n|)$ . We consider the following cases:

- If  $n$  is not of the form  $2^k$  or  $2^k + 1$ , by lemma 4.4 we have  $|\ker R| = 2$ , hence  $\text{val}_2(|\widehat{A}_n|) = \text{val}_2(|\widehat{S}_n|) - 1 \geq \text{val}_2(|S_n|) - 1 = \text{val}_2(|A_n|)$ .
- If  $n \leq 3$ ,  $A_n$  is abelian.
- If  $n = 4$ ,  $A_n[2^\infty]$  is an abelian group of size 4 (the Klein 4-group), hence  $\widehat{A}_n[2^\infty]$  has 4 elements.
- If  $n = 5$ , we take the natural embedding  $A_4 \hookrightarrow A_5$  (where the permutations in the image fix the number 5). Then, one may extend the elements of  $\widehat{A}_4[2^\infty]$  constructed above to  $\widehat{A}_5[2^\infty]$  by setting the functions to be 1 outside of  $\widehat{A}_4[2^\infty]$ . This shows that  $\text{val}_2(|\widehat{A}_5|) \geq 2 = \text{val}_2(|A_5|)$ .
- If  $n = 2^k + \epsilon$ , where  $\epsilon \in \{0, 1\}$  and  $k \geq 3$ , let  $m = 2^k$ . We will construct elements of  $\widehat{A}_n[2]$  by a small variation on the proof of theorem 4.2: Let  $A$  be the set of  $m/4$ -cycles in  $S_n$ , with the equivalence relation defined by  $\pi \sim \pi^i$  for  $\sigma \in A$  and odd  $i$ , and let  $V$  be the  $\mathbb{F}_2$ -vector space of functions  $f : A \rightarrow \mathbb{F}_2^+$  satisfying  $f(\pi^i) = i \cdot f(\pi)$  for odd  $i$ . We have  $\dim_{\mathbb{F}_2}(V) = |A/\sim|$ . For any  $f \in V$ , we extend  $f$  to a function  $\tilde{f} : A_n[2^\infty] \rightarrow \mathbb{F}_2^+$  by  $\tilde{f}(\pi) = \sum_{c \in c(\pi^2, m/4)} f(c)$ , where  $c(-, -)$  is as in the proof of theorem 4.2. We claim that  $\tilde{f} \in \widehat{A}_n[2^\infty][2]$ . Indeed, let us assume that  $\pi_1, \pi_2 \in A_n[2^\infty]$  commute, and let  $\pi_3 = \pi_1\pi_2$ . Since  $\pi_i \in A_n$ , no  $\pi_i$  is an  $m$ -cycle. If no  $\pi_i$  contains an  $m/2$ -cycle, then no  $\pi_i^2$  contains an  $m/4$ -cycle, hence  $\tilde{f}(\pi_i) = 1$  for all  $i$ , and  $f(\pi_3) = f(\pi_1)f(\pi_2)$ . If  $\pi_1$  contains an  $m/2$ -cycle  $\sigma_1$ , then  $\pi_2$  (acting by conjugation) either fixes  $\sigma_1$  or moves it to an additional  $m/2$ -cycle of  $\pi_1$ . Hence,  $\pi_2^2$  fixes  $\sigma_1$ . Consequently, there exists  $k$  such that  $\pi_2^2$  is equal to  $\sigma_1^k$  on the support of  $\sigma_1$ . Since  $\pi_2$  is not an  $m$ -cycle,  $k$  must be even. We conclude that  $\pi_2^2$  is a power of  $\pi_1^2$  on the support of any  $m/4$ -cycle of  $\pi_1^2$ , and similarly that  $\pi_i^2$  is a power of  $\pi_j^2$  on the

support of any  $m/4$ -cycle of  $\pi_j$ , for all  $i, j \in \{1, 2, 3\}$ . Hence, there exist disjoint cycles  $c_1, \dots, c_u$  and integers  $a_{ij}$  such that  $\pi_i|_{\text{supp}(c_j)} = c_j^{a_{ij}}$ , and any  $m/4$ -cycle of any  $\pi_i$  is supported on  $\text{supp}(c_j)$  for some  $j$ . From here, it follows that  $\tilde{f}(\pi_3) = \tilde{f}(\pi_1)\tilde{f}(\pi_2)$ . We conclude, using lemma 2.5, that  $\dim_{F_2} \widehat{A}_n[2] \geq \dim_{\mathbb{F}_2} V = \binom{n}{m/4} \frac{(m/4-1)!}{(m/4-m/8)} \geq n \geq \text{val}_2(|A_n|)$ .

□

## 5. UNIPOTENT GROUPS

For groups of unipotent upper triangular matrices, we will construct semicharacters by a discrete version of the log function.

**Definition 5.1.** For all  $n$  and prime  $p$ , let  $w_{n,p}$  be the polynomial

$$w_{n,p}(x) = \sum_{i=1}^{n-1} (-1)^{i+1} \frac{p^e}{i} x^i \in \mathbb{Q}_{(p)}[x]$$

where  $e$  is the number satisfying  $p^e \leq n-1 < p^{e+1}$ .

Note that modulo  $p$ ,  $w_{n,p}(x) \equiv \sum_{ip^e < n} (-1)^{i+1} \frac{x^{ip^e}}{i}$ .

**Lemma 5.2.** Let  $p$  be prime, and let  $A$  be a nilpotent  $\mathbb{F}_p$ -algebra of nilpotence degree  $n$ .

(1) If  $x, y \in A$  commute then

$$w_{n,p}(x + y + xy) = w_{n,p}(x) + w_{n,p}(y).$$

(2) If  $p \geq n$  then  $w_{n,p}$  defines a bijection from  $A$  to itself.

*Proof.*

(1) We have the formal identity over  $\mathbb{Q}$ ,

$$\sum_{i \geq 1} (-1)^{i+1} \frac{(x + y + xy)^i}{i} = \log((1+x)(1+y)) = \log(1+x) + \log(1+y) = \sum_{i \geq 1} (-1)^{i+1} \left( \frac{x^i}{i} + \frac{y^i}{i} \right)$$

We multiply it by  $p^e$ , and take the resulting identity modulo monomials of degree  $\geq n$ . If  $I$  is the ideal in  $\mathbb{Q}[x, y]$  generated by these monomials, we get an identity in  $\mathbb{Q}[x, y]/I$ ,

$$w_{n,p}(xy + x + y) = w_{n,p}(x) + w_{n,p}(y).$$

Since all the coefficients are in  $\mathbb{Q}_{(p)}$ , and  $A$  is an  $\mathbb{F}_p$ -algebra, the identity holds for any two commuting elements in  $A$ .

- (2) Since  $p \geq n$ , we have  $e = 1$ . let  $u(x) = \sum_{i=1}^{n-1} \frac{x^i}{i!}$ . By the formal identity  $\exp(\log(1+x)) - 1 = x$ , we get, by the same argument, that  $u(w(x)) = x$  for all  $x \in A$ .

□

**Theorem 5.3.** *Let  $\mathbb{F}$  be a finite field, let  $n \leq \text{char}(\mathbb{F})$ , and let  $G = U(n, \mathbb{F})$  be the group of upper triangular unipotent matrices. Then, conjecture 1.1 holds for  $G$ .*

*Proof.* Let  $N$  be the additive group of nilpotent upper triangular matrices in  $M_n(\mathbb{F})$ . We define the map  $\log : G \rightarrow N$  by  $\log(A) = w(A - I)$ . By lemma 5.2,  $\log$  is a bijection, and if  $A, B$  commute then  $\log(AB) = \log(A) + \log(B)$ . Thus, the map  $\hat{N} \rightarrow \hat{G}$  given by  $\phi \mapsto \phi \circ \ln$  is a monomorphism, hence  $|\hat{G}|$  is divisibly by  $|N| = |G|$ . □

## 6. GENERAL LINEAR GROUPS

In this section, we consider the case of  $G = GL(n, q)$  where  $q$  is a power of a prime  $p$ , and prove conjecture 1.1 for it. Naturally, the cases  $l = p$  and  $l \neq p$  are completely different from one another. We start with  $l \neq p$ . The  $l$ -Sylow groups of  $G$  are described in [1]. In the case  $l|q-1$  the description is the simplest one: an  $l$ -Sylow subgroup can be embedded in the group of monomial matrices (that is, matrices that have exactly one nonzero entry in each row). We call this group  $M$ , and assume that  $L \leq M$  is an  $l$ -Sylow subgroup of  $G$ .

**Lemma 6.1.** *Assume that  $l|q-1$ ,  $n = l^e$ , and let  $g \in G[l^\infty]$  be an element of maximal order.*

- (1) *If  $h \in G[l^\infty]$  commutes with  $g$  then  $h$  is a power of  $g$ .*
- (2) *The action of  $g$  on the vector space  $V := \mathbb{F}_q^n$  makes  $V$  an irreducible  $g$ -module.*

*Proof.* (1) We may assume, without loss of generality, that  $g, h \in L$ . We have a natural homomorphism  $\pi : M \rightarrow S_n$ . Since  $g$  is of maximal order in  $L$ ,  $\pi(g)$  is cyclic. Hence, there exists  $t$  such that  $\pi(h) = \pi(g)^t$ . We may assume without loss of generality that  $\pi(g) = (12..n)$ . Let  $S$  be the permutation matrix corresponding to  $\pi(g)$ . There exist diagonal matrices  $D_1 = \text{diag}(x_1, \dots, x_n)$  and  $D_2 = \text{diag}(y_1, \dots, y_n)$  such that  $g = SD_1, h = S^t D_2$ . From  $gh = hg$  we get that  $x_{i-t}y_i = y_{i-1}x_i$  for all  $i$  (with indices modulo  $n$ ), or  $\frac{y_i}{y_{i-1}} = \frac{x_i}{x_{i-t}}$ , hence  $h$  is determined up to a scalar multiple, hence  $h$  is a scalar multiple of  $g^t$ , say  $h = cg^t$ . Since  $g$  and  $h$  are of  $l$ -power order, so is  $c$ . Since  $g$  is of maximal order,  $g^n = dI$  and  $d$  is of maximal order in  $\mathbb{F}_q^*[l^\infty]$ . Since  $\mathbb{F}_q^*$  is cyclic,  $c$  is a power of  $d$ , hence  $cI$  is a power of  $g$ , and so is  $h$ .

(2) Let us still assume, without loss of generality, that  $\pi(g) = (12..n)$ . Moreover, by conjugating with diagonal matrices, we may assume that  $g$  represents the linear transformation  $(x_1, \dots, x_n) \rightarrow (cx_n, x_1, x_2, \dots, x_{n-1})$ , where  $c \in \mathbb{F}_q$  is an element of order  $l^r$ , and  $l^r|q-1$ . By Maschke's theorem,  $\mathbb{F}_q[g]$  is a semisimple ring.



If  $V$  had a nontrivial  $\mathbb{F}_q[g]$ -submodule, then there would be a decomposition  $V = V_0 \oplus V_1$  where  $V_i$  are nontrivial and  $g$ -invariant. Then, we could write  $g = g_0 g_1$  where each  $g_i$  is equal to  $g$  on  $V_i$  and to the identity on  $V_{1-i}$ . Both  $l_0, l_1$  commute and are of  $l$ -power order, hence by part 1,  $g_0$  is a power of  $g$ , say  $g_0 = g^i$  with  $0 < i < l^{e+r}$ . Thus, we will arrive at a contradiction by showing that for such  $i$ ,  $g^i$  has no nonzero fixed vector. Suppose that  $v$  is such a vector, and that  $t > 0$  is minimal such that  $g^t v = v$ . Then,  $g^{l^{e+r}+it} v = v$  for all  $i$ , hence  $t$  divides  $l^{e+r}$ , i.e.  $t = l^u$  with  $0 \leq u < e + r$ .

If  $u \leq e$ , then we have

$$(x_1, \dots, x_n) = g^t(x_1, \dots, x_n) = (cx_{n-t+1}, \dots, cx_n, x_1, \dots, x_{n-t})$$

Hence, for all  $1 \leq j \leq t$ ,

$$x_j = x_{j+t} = x_{j+2t} = \dots = x_{j+n-t} = c^{-1}x_j$$

And we get  $x_j = 0$  for all  $j$ .

If, on the other hand,  $e < u < e + r$ , then since  $g^{l^e} = c \cdot I$ , we have  $g^t = c^{l^{u-e}} \cdot I$ , and this map has no nonzero fixed vectors. Again, we get a contradiction.  $\square$

**Lemma 6.2.** *If  $l|q-1$  Then  $\text{val}_l(|\hat{G}|) \geq \text{val}_l(G)$*

*Proof.* Let  $e$  be such that  $l^e \leq n < l^{e+1}$ , and as before, assume that  $l^r || q-1$ . Since the  $l$ -Sylow subgroup  $L$  is contained in the group of monomial matrices  $M$ , the maximal order of an element in  $G[l^\infty]$  is  $l^{e+r}$ . Moreover, each element in  $G[l^\infty]$  acts on  $V = \mathbb{F}_q^n$ . By Maschke's theorem,  $V$  can be decomposed to irreducibles, and by the structure of matrices in  $M[l^\infty]$ , the dimensions of the components are bounded by  $l^e$ .

Let  $A$  be the set of pairs  $(W, T)$  where  $W$  is a vector subspace of  $V$  of dimension  $l^e$ , and  $T \in GL(W)$  is of order  $l^{e+r}$ . By lemma 6.1, if  $(W, T) \in A$  then  $W$  is an irreducible  $\mathbb{F}_q[T]$ -module. Define an equivalence relation  $\sim$  on  $A$  by setting  $(W, T) \sim (W, T^i)$  for all  $(W, T) \in A$  and  $i$  prime to  $l$ . Let  $U$  be the group of functions  $u : A \rightarrow \mathbb{F}_l^+$  such that  $u(W, T^i) = iu(W, T)$  for  $i$  prime to  $l$ . We have  $\dim_{\mathbb{F}_l} U = |A|/\sim$ . For each  $g \in G[l^\infty]$ , let  $\text{irr}(g)$  be the set of subspaces  $W$  of  $V$  such that  $gW = W$  and  $(W, g|_W) \in A$ . Any element  $u$  of  $U$  induces a function  $f_u : G[l^\infty] \rightarrow \mathbb{F}_l^+$  defined by

$$f_u(g) = \sum_{W \in \text{irr}(g)} u(W, g|_W).$$

Let us prove that if  $g, h \in G[l^\infty]$  commute then  $f_u(gh) = f_u(g) + f_u(h)$ . Indeed, if  $W$  is  $g$ -invariant then so is  $hW$ . Hence,  $h$  acts on the set of  $g$ -invariant irreducible subspaces of  $V$  of dimension  $l^e$ , and since

the orbits are of  $l$ -power size and  $l^{e+1} > n$ ,  $h$  fixes each such subspace. By lemma 6.1, we conclude that if  $W \in \text{irr}(g)$  then  $hW = W$  and  $h|_W$  is a power of  $g|_W$ . Consequently, for each  $W \in \text{irr}(g) \cup \text{irr}(h) \cup \text{irr}(gh)$ , we have  $u(W, gh) = u(W, g) + u(W, h)$ , where  $u(W, x)$  is defined to be 0 if  $(W, x) \notin A$ .

By lemma 2.5,  $f_u$  has a unique extension to an element of  $\widehat{G}[l]$ . We conclude that  $\dim_{\mathbb{F}_l} \widehat{G}[l] \geq |A/\sim|$ . We will be done by showing that  $|A/\sim| \geq \text{val}_l(|G|)$ .

For  $\text{val}_l(|G|)$ , we have the estimate

$$\text{val}_l(|G|) = \text{val}_l(|M|) = \text{val}_l((q-1)^n n!) \leq \frac{n}{l-1} + nr \leq n(r+1) \leq 2nr.$$

For  $|A/\sim|$ , We have two cases:

- If  $n = l^e$  then we have  $(n-1)!(q-1)^{n-1}l^r(1-\frac{1}{l})$  monomial matrices  $g$  of order  $l^{e+r}$ : One has to choose a cyclic permutation of order  $n$ , and  $n$  nonzero entries  $\alpha_1, \dots, \alpha_n$  of the matrix such that  $\prod \alpha_i$  is an element of order  $l^r$  in  $\mathbb{F}_q^*$ . This gives a matrix  $g$  satisfying  $g^{l^e} = \prod \alpha_i$ , hence its order is  $l^{e+r}$ , and  $(V, g) \in A$ . Hence,

$$|A/\sim| \geq \frac{(n-1)!(q-1)^{n-1}l^r(1-\frac{1}{l})}{l^{r+e}(1-\frac{1}{l})} = \frac{(n-1)!}{n}(q-1)^{n-1} \geq \frac{1}{2} \cdot 2^{r(n-1)} \geq 4r(n-1) \geq 2nr.$$

We have used the inequality  $2^x \geq 8x$  which holds for  $x \geq 6$ . If  $r(n-1) \leq 6$ , then  $2nr \leq 24$ . We have  $\frac{(n-1)!}{n}(q-1)^{n-1} \geq 24$  except for the following values of  $n$  and  $q$ :  $n = 2$  and  $q \leq 47$ ,  $n = 3$  and  $q \leq 7$ ,  $n = 4$  and  $q = 3$ . For these cases, the inequality  $\frac{(n-1)!}{n}(q-1)^{n-1} \geq \text{val}_l(n!) + nr$  holds, except when  $n = 2$  and  $q \in \{3, 5, 9, 17\}$ . For these cases, it is easy to see, by counting group elements of order  $l^{e+r}$ , that  $|A/\sim| \geq \text{val}_l(|G|)$ .

- If  $n \neq l^e$  then the number of subspaces  $W$  of dimension  $l^e$  is at least the number of one dimensional subspaces, i.e.  $\frac{q^n-1}{q-1}$ . On each such space, we have at least  $(l^e-1)!l^{rl^e}(1-\frac{1}{l})$  transformations of order  $l^{e+r}$ . Hence,

$$|A/\sim| \geq \frac{(1+q+\dots+q^{n-1})l^{rl^e}(1-\frac{1}{l})}{l^{e+r}(1-\frac{1}{l})}$$

We have  $l^{rl^e-e-r} \geq l^{r(e-e-r)} \geq 1$  and

$$1+q+\dots+q^{n-1} \geq q^{n-2}+q^{n-1} \geq 2^{r(n-2)}+2^{r(n-1)} \geq 2r(n-2)+2r(n-1).$$

If  $n > 2$  then  $(n-2) + (n-1) \geq n$ , hence  $|A/\sim| \geq 2rn$ .

If  $n = 2$  then  $\text{val}_l(|G|) \leq 1+2r \leq 1+2^r \leq 1+l^r \leq q \leq |A/\sim|$ .

□

Now, consider the general case where  $l \neq p$  is any divisor of  $|G|$ . Let  $d$  be minimal so that  $l|q^d - 1$ , and we write  $n = n_0d + n_1$ ,  $0 \leq n_1 < d$ . We consider the embedding  $GL(n_0, q^d) \subset GL(n_0d, q)$  by restriction of scalars. By [1], remark 2.5, any  $l$ -Sylow subgroup of  $GL(n_0, q^d)$  is also an  $l$ -Sylow subgroup of  $G$ , through the embedding. We denote by  $M$  the image of the group of monomial matrices of  $GL(n_0, q^d)$  in  $G$ , and let  $L$  be an  $l$ -Sylow subgroup contained in  $M$ . Generalizing lemma 6.1, we have

**Lemma 6.3.** *Assume that  $n_1 = 0, n_0 = l^e$ , and let  $g \in G[l^\infty]$  be an element of maximal order.*

- (1) *If  $h \in G[l^\infty]$  commutes with  $g$  then  $h$  is a power of  $g$ .*
- (2) *The action of  $g$  on the vector space  $V := \mathbb{F}_q^n$  makes it an irreducible  $g$ -module.*

*Proof.* (1) Since  $h, g$  lie in a common  $l$ -Sylow subgroup, we may assume that  $h, g \in M$ . Hence, the claim follows from lemma 6.1.

(2) Let  $l^r || q^d - 1$  and assume that  $g \in M$ . The maximal order of an element in  $M[l^\infty]$  is  $l^{e+r}$ . In particular, this is the order of  $g$ . By lemma 6.1,  $V$  is irreducible as an  $\mathbb{F}_{q^d}[g]$ -module. Since as an element of  $GL(n_0, q^d)$ ,  $g^{l^e}$  is a scalar matrix, and the scalar is a generator of the field extension  $\mathbb{F}_{q^d}/\mathbb{F}_q$ ,  $V$  is also irreducible as an  $\mathbb{F}_q[g]$ -module.  $\square$

**Lemma 6.4.** *For any  $l \neq p$  dividing  $|G|$ ,  $val_l(|\widehat{G}|) \geq val_l(G)$ .*

*Proof.* By the description of the  $l$ -Sylow subgroups, and by lemma 6.3, the maximum dimension for an irreducible invariant space of  $g \in G[l^\infty]$  is  $l^e d$ . Note that  $l^e d \leq n_0 d \leq n$  and  $l^{e+1} d > n$  (because if  $l^{e+1} d \leq n$ , then since  $n < n_0 d + d$ ,  $l^{e+1} d < n_0 d + d \Rightarrow l^{e+1} < n_0 + 1 \Rightarrow l^{e+1} \leq n_0$ , contradiction).

Hence, we may use the proof technique of lemma 6.2: Let  $A$  be the set of pairs  $(W, T)$  where  $\dim T = l^e d$  and  $T \in GL(W)$  is of the maximal order  $l^{e+r}$ . Define an equivalence relation on  $A$  by  $(W, T) \sim (W, T^i)$  when  $(i, l) = 1$ . The same arguments show that  $\dim_{\mathbb{F}_l} \widehat{G}[l] \geq |A / \sim|$ . We have seen in the proof of lemma 6.2 that  $|A / \sim| \geq val_l|M|$ . Since  $val_l|G| = val_l|M|$ , we are done.  $\square$

Finally, let us treat the case  $l = p$ .

**Lemma 6.5.**  $val_p(|G^*|) \geq 2val_p(|G|)$ .

*Proof.* Let  $N$  be the algebra of upper triangular nilpotent  $n$  by  $n$  matrices, and let  $U = I + N$  be the unipotent group.  $U$  is a  $p$ -Sylow subgroup of  $G$ . We define a function  $F : G[p^\infty] \rightarrow M(n, q)$  by  $F(g) = w_{n,p}(g - 1)$ , where the polynomial  $w_{n,p}$  was defined before lemma 5.2. Note that  $F(hgh^{-1}) = hF(g)h^{-1}$ . If  $x, y \in G[p^\infty]$  commute, then they lie in a common Sylow subgroup, hence we may assume that they lie in  $U$ . Let  $a = x - I, b = y - I$ , then  $a, b \in N$ . By lemma 5.2,

$$F(xy) = F((I + a)(I + b)) = w_{n,p}(ab + a + b) = w_{n,p}(a) + w_{n,p}(b) = F(I + a) + F(I + b) = F(x) + F(y).$$

We will denote by  $F(g)_{ij}$  the  $(i, j)$  entry of  $F(g)$ . Given any  $n^2 - n$  linear functionals  $(\phi_{ij} \in \text{Hom}_{\mathbb{F}_p}(\mathbb{F}_q, \mathbb{F}_p))_{1 \leq i \neq j \leq n}$ , the function  $T_{(\phi_{ij})} : G[p^\infty] \rightarrow \mathbb{F}_p^+$  defined by  $T_{(\phi_{ij})}(g) = \sum_{i \neq j} \phi_{ij}(F(g)_{ij})$  is in  $\widehat{G[p^\infty]}[p]$ , and by lemma 2.5 extends to an element of  $\widehat{G}[p]$ . Let us see that in this way, we get a subspace of  $\widehat{G}[p]$  of dimension  $\dim(\mathbb{F}_q/\mathbb{F}_p)(n^2 - n) = 2\text{val}_p(|G|)$ : Indeed, any matrix of the form  $aE_{ij}$  (where  $E_{ij}$  is the elementary matrix with only one nonzero entry 1 at  $(i, j)$ ) for  $i \neq j$  is in the image of  $F$ , because if  $d$  is the least degree in the polynomial  $w_{n,p} \bmod p$ , and  $M$  is the nilpotent matrix

$$\begin{pmatrix} 0 & a & & & & \\ & 0 & 1 & & & 0 \\ & & \ddots & \ddots & & \\ & & & 0 & 1 & \\ & & & & 0 & 0 \\ & 0 & & & \ddots & \ddots \\ & & & & & 0 & 0 \\ & & & & & & 0 \end{pmatrix}$$

with  $d - 1$  1's, then  $w_{n,p}(M) = M^d$  has only one nonzero entry equal to  $a$ , and by conjugating we get a matrix  $A$  satisfying  $F(I + A) = w_{n,p}(A) = aE_{ij}$ . Hence, if  $T_{(\phi_{ij})} \equiv 0$  then  $\phi_{ij} = 0$  for all  $i \neq j$ .  $\square$

We conclude:

**Theorem 6.6.** *For all  $n, q$ , conjecture 1.1 holds for  $GL(n, q)$ .*

**Corollary 6.7.** *If  $(n, (q - 1)) = 1$  then conjecture 1.1 holds for  $SL(n, q) = PSL(n, q)$ .*

*Proof.* If  $\phi$  is in the kernel of the restriction map  $R : \widehat{GL(n, q)} \rightarrow \widehat{SL(n, q)}$ , then since for every  $g \in GL(n, q)$  there is a scalar  $c \in \mathbb{F}_q^*$  such that  $c^{-1}g \in SL(n, q)$ , we have  $1 = \phi(c^{-1}g) = \phi(cI)^{-1}\phi(g) \Rightarrow \phi(g) = \phi(cI)$ .

We get an isomorphism  $\ker R \cong \mathbb{F}_q^*$  by  $\phi \rightarrow \phi \circ \det$ . Hence,  $\frac{|\widehat{SL(n, q)}|}{|\widehat{SL(n, q)}|} = \frac{|\widehat{GL(n, q)}|/(q-1)}{|\widehat{GL(n, q)}|/(q-1)} \in \mathbb{N}$ .  $\square$

## REFERENCES

- [1] AlAli, Mashhour I.; Hering, Christoph; Neumann, Anni, A number theoretic approach to Sylow  $r$ -subgroups of classical groups. (English summary) Rev. Mat. Complut. 18 (2005), no. 2, 329–338.
- [2] Kimmerle, Wolfgang; Lyons, Richard; Sandling, Robert; Teague, David N. Composition factors from the group ring and Artin's theorem on orders of simple groups. Proc. London Math. Soc. (3) 60 (1990), no. 1, 89–122.

Department of Mathematics and Computer Science, The Open University of Israel, 1 University Road, p.o. box 808, Raanana, Israel.

E-mail address: [gilal@openu.ac.il](mailto:gilal@openu.ac.il)